RFDIDS: Radio Frequency-based Distributed Intrusion Detection System for the Power Grid

Tohid Shekari, Christian Bayens, Morris Cohen, Lukas Graber, and Raheem Beyah
School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, USA
t.shekari@gatech.edu, cbayens3@gatech.edu, mcohen@gatech.edu, lukas.graber@ece.gatech.edu, rbeyah@ece.gatech.edu

Abstract—**Recently, the number of cyber threats on power systems has increased at an unprecedented rate. For instance, the widespread blackout in Ukrainian power grid on December 2015 was a wakeup call that modern power systems have numerous vulnerabilities, especially in power substations which form the backbone of electricity networks. There have been significant efforts among researchers to develop effective intrusion detection systems (IDSs) in order to prevent such attacks or at least reduce their damaging consequences. However, all of the existing techniques require some level of trust from components on the supervisory control and data acquisition (SCADA) network; hence, they are still vulnerable to sophisticated attacks that can compromise the SCADA system completely. This paper presents a radio frequency-based distributed intrusion detection system (RFDIDS) which remains reliable even when the entire SCADA system is considered untrusted. The proposed system uses radio frequency (RF) emissions to monitor the power grid substation activities. Indeed, it utilizes a radio receiver as a diagnostic tool to provide air-gapped, independent, and verifiable information about the radio emissions from substation components, particularly at low frequencies (LF, 0.05−50 kHz, or $>$20 μs period). The simulation and experimental results verified that four types of diagnostic information can be extracted from radio emissions of power system substation circuits: i) harmonic content of the circuit current, ii) fundamental frequency of the circuit current, iii) impulsive signals from rapid circuit current changes, and iv) sferics from global lightning strokes. Each or a combination of the first three diagnostics can be effectively leveraged to directly detect specific types of power grid attacks. Meanwhile, the last diagnostic is utilized to check the integrity of the receiver's signal as it is encoded with the quasi-random distribution of the global lightning strokes. The simulation and real-world experimental results verified the effectiveness of RFDIDS in protecting the power grid against sophisticated attacks.**

I. Introduction

A. Aim and Motivation

The electricity grid is a highly complex control system and is one of the most impressive engineering feats of the modern era. Modern societies critically rely on the proper operation of power delivery systems in nearly every facet [1]–[3]. There are a number of threats to the reliability and security of the electric grid, including space weather, aging, accidents, and random failures. In this paper, we focused on the growing threat from cyberattacks to substations.

The world's first known successful cyberattack on a power system is the Ukrainian power grid attack which took place on December 23, 2015. During this event, the attackers used spearphishing in order to gain access to the supervisory control and data acquisition (SCADA) system of multiple substations by posing as a trusted entity [4]. Following the attack, circuit breakers in 30 substations were switched off, and more than 230,000 residents were left without power [5], [6]. At the same time, the attackers spoofed the SCADA network traffic and reported a normal operating condition to the control center. A key aspect of the incident was a distributed denial of service (DDoS) attack on the call centers so that customer complaints could not be received by the power company. Between this and the spoofing of network traffic, the company was unaware of the attack until it was too late. By this point, the substations were shut off and would not accept commands from the power company to come back online [4].

After this attack, the number of power outages due to cyberattacks has increased dramatically. Ukrainian power grid blackout in 2016 as well as the discovery of Dragonfly 2.0 as a root cause for a set of outages in the US, Turkey, and Switzerland are testimonies to this claim [5]–[8]. Prior to 2013, Dragonfly targeted defense and aviation companies in the US and Canada. Additionally, the recent attacks on the US power grid by Russia are a sobering wake up call that the power grid needs securing [9]–[11]. The aforementioned attacks on power systems mainly focused on substations, which form the backbone of electricity networks. Substations offer a large attack surface as they are widely distributed throughout the power networks. As an illustrative example, there are ∼70,000 substations across the US [12].

To detect attacks early and potentially reduce their damaging consequences, we need a reliable and robust intrusion detection system (IDS) for the power grid. The existing IDSs focused on securing power substations through monitoring the network traffic of the SCADA system. Accordingly, if the attacker can compromise the SCADA network entirely, the IDS will not be able to detect his malicious activities in the substation. Motivated by this fact, the aim of this paper is to propose an air-gapped distributed IDS which monitors the substation activities by radio frequency (RF) measurements (as a side channel) to verify the correctness of the SCADA network traffic. With this approach, the SCADA system is assumed to be an untrusted entity.

Network and Distributed Systems Security (NDSS) Symposium 2019
24-27 February 2019, San Diego, CA, USA
ISBN 1-891562-55-X
https://dx.doi.org/10.14722/ndss.2019.23462
www.ndss-symposium.org

B. Related Work

Attacks on the power grid can be classified as four groups based on the end goal of the attackers: i) false data injection [13], ii) malicious command injection [6], iii) communication delay attack [14], and iv) impersonation of control center [4]. The first two groups are common and were implemented during the Ukrainian power grid blackout in 2015 [4]. In this event, the attacker opened the substation circuit breakers and cut the power to customers while feigning normal operating condition to the control center.

Power system cyber security has been traditionally handled using network security and Internet technology (IT) practices [15]–[28]. The common features of these works include: i) they obtain the SCADA system measurements as an input, and ii) they leverage machine learning methods that look for statistical anomalies in a feature space (often heuristic and require significant training). For instance, the authors of [20] proposed a hybrid IDS that learns temporal state-based specifications for different possible scenarios in the system (disturbances, normal control operations, and cyberattacks). A data mining approach is then adopted to learn patterns for various scenarios.

While there are a variety of companies selling industrial control system (ICS)-specific IDSs and intrusion prevention systems (IPSs), Snort [29] is a popular free and open-source solution for power grid applications. Using Snort, researchers can define rules to detect various types of attacks. For instance, specific rules can be defined to alert operators of attackers performing reconnaissance by detecting suspected SSH password guessing, network scanning, and Modbus scanning.

However, the challenge is that power system security goals differ from traditional IT security ones due to additional requirements and conditions of operation [30]. The interconnection of the physical world and cyber world is a unique feature of modern power grids compared to traditional IT infrastructures. Therefore, most of the aforementioned solutions are still vulnerable because they: i) rely on the very components of the grid they seek to protect (e.g., sensors that monitor power grid equipment), ii) are directly connected to the power grid (and thus are "in the line of fire"), and iii) rely on the network being monitored to transport authentic security alerts. Accordingly, it is still theoretically possible that the solutions themselves can be compromised. This partially motivates the need for security solutions that are completely decoupled from the system they monitor.

Purely cyber processes can be monitored directly through physical channels, since they emit physical emanations of different modalities. Past efforts using physical channels (decoupled from the systems being monitored) illustrate the feasibility of targeted secret information disclosure (e.g., cryptographic keys) and signal probes [31]–[33]. These works explore technologies to associate the running state of a physical device with its involuntary analog emissions across different physical modalities. Electromagnetic emissions, acoustic emanations, power fluctuations, and thermal output variations are the main physical modalities used in previous works. In this paper, we will use the RF emissions of the substation circuits to detect malicious activities of attackers. The machine learning-based studies presented in [34]–[36] have leveraged high frequency electromagnetic emissions emanated from processors of computers and embedded devices to monitor the program execution path. Our approach has the following distinguishing features from the aforementioned works: i) our method utilizes the magnetic field measurements at low frequencies, ii) we extracted the direct mathematical equations that can reconstruct the flowing current in substation circuits from the magnetic field signal, iii) the proposed scheme itself is robust against spoofing/replay attacks as the measured signal is encoded with the quasi-random distribution of lightning strokes around the globe, and iv) we directly monitor the physical components of the power grid since the ultimate goal of the attacker is to influence the system physical behavior.

C. Contributions

A radio frequency-based distributed intrusion detection system (RFDIDS) is proposed in this paper to quickly detect cyberattacks in power system substations. The basic idea behind the novel approach is that any AC circuit in a substation invariably emits a magnetic field which our receiver can very easily detect. Our antenna setup reliably captures four useful attributes of the magnetic field in power substations: i) magnetic field harmonic content (circuit current harmonic content), ii) magnetic field fundamental frequency (system fundamental frequency), iii) magnetic field impulsive emissions (impulses in the circuit current caused by switching actions), and iv) lightning sferics. The useful information that can be extracted from each of the first three attributes were mentioned inside the parenthesis. The first three quantities measured by our system will be compared to the SCADA network traffic, hence providing an air-gapped and redundant mechanism to power system monitoring and diagnostics. Circuit breaker malicious switching, transformer malicious tap changing, false data injection to protective relays, and control center are the most important attacks which can be detected by RFDIDS. We also utilize a unique and novel method to authenticate the collected data using the quasi-random sequence of global lightning encoded into the magnetic field data (last mentioned attribute), meaning that low frequency (LF) magnetic field data cannot be spoofed/played back by an attacker. As the proposed system is non-invasive, it can be easily augmented onto existing substations. This system can be realized as an extension of an existing open source IDS such as Snort. Indeed, it can act as a complementary physical signal-based diagnostic and can be codified as a Snort module. The salient features of the proposed methodology are summarized as follows:

- RFDIDS is air-gapped from the power system substation components and uses a side channel (RF emissions) to estimate the operating status of the substation;
- The developed methodology can protect the power grid against attacks that can compromise the entire grid and all of its attached components;
- The measured signal from the side channel cannot be spoofed/played back as it is encoded with the impulses from lightning strokes occurred in far distances.

These features make RFDIDS robust and resilient against advanced types of attacks in which the attackers can simultaneously compromise the SCADA and RF measurement systems.

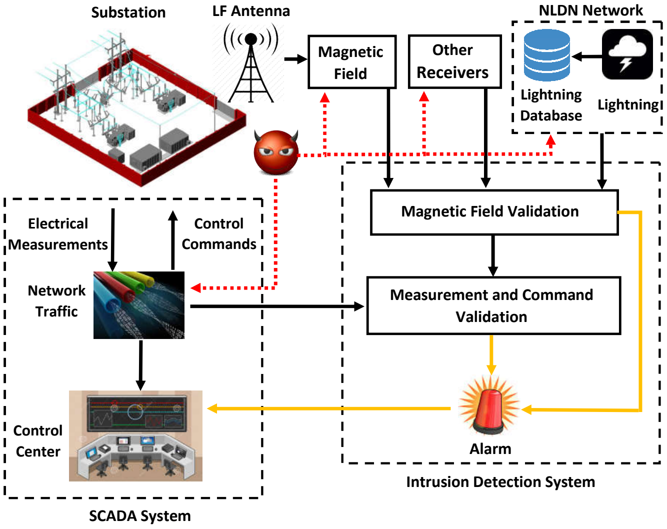


Fig. 1. The overall structure of RFDIDS.

The rest of this paper is organized as follows. The threat model and the overview of the proposed scheme is given in Section II. Section III presents the background information about the power grid, RF measurements, and lightning authentication scheme. The detailed methods to extract useful data from RF measurements in substations will be explained in Section IV. Section V represents simulation and experimental results to verify the effectiveness of the proposed approach. The robustness and resilience of the new method in challenging situations are thoroughly discussed in Section VI. Finally, the conclusion and possible directions are given in Section VII.

II. Threat Model and Scheme Overview

An overview of the considered threat model and RFDIDS structure is illustrated in Fig. 1. As shown in this figure, RFDIDS has four inputs: i) magnetic field data from the LF receiver (located inside the substation fences), ii) lightning database signal, iii) lightning signals from the receivers located in nearby substations, and iv) measurements from the SCADA system and direct sensors. Also, the global positioning system (GPS) signal is used to synchronize the inputs of RFDIDS with each other. In the first step, the integrity of the LF antenna signal is checked using first three inputs and the method described in Section III-C. If the signal integrity is verified, the second step will be executed; otherwise, an alarm, as a sign of intrusion, is sent to the control center via a secure mobile backchannel separate from the SCADA communications, and the substation control changes to manual mode. In the second step, RFDIDS extracts the substation measurements and control actions from the SCADA network traffic and antenna signal (i.e., the method described in Section IV). If there is any inconsistency between these two, RFDIDS will set the alarm signal and changes the substation control to manual mode to prevent further potential adversary actions.

The main assumptions of the threat model are: i) the SCADA system is totally compromised by the attacker, and hence, is untrusted, ii) a knowledgeable attacker will be fully aware of the substation configuration, its control mechanisms, and even our algorithm, and iii) GPS is a secure and trusted entity[1]. In this paper, the possible attacker is classified into four main groups:

- Attacker level 1: This attacker has background in ICS/SCADA security but he has no knowledge on electromagnetic analysis;
- Attacker level 2: This attacker has background in both ICS/SCADA security and electromagnetic analysis;
- Attacker level 3: This attacker has background in both ICS/SCADA security and electromagnetic analysis as well as complete knowledge of and access to the lightning database;
- Attacker level 4: This attacker has background in both ICS/SCADA security and electromagnetic analysis as well as complete knowledge of and access to the lightning database and geographical information about the power grid.

Each of these attackers and possible defense mechanisms are discussed in below.

A. *Attacker Level 1*

This attacker can only compromise the SCADA system. Therefore, the SCADA system is assumed to be completely untrusted. However, the magnetic field measurement signal from the LF antenna, the global lightning database, and sferics detected from other LF antennas remain trusted entities. The attack is carried out such that the substation equipment behaves maliciously despite sending legitimate measurements to the control center. For instance, the attacker opens a distribution line circuit breaker to cut the electricity to customers while sending the circuit breaker close status to the control center. The attacker can launch a DDoS attack on the call centers so that customer complaints do not reach the power company (as was done during the Ukrainian power grid blackout in 2015 [5], [6]). Consequently, the power company is unaware of the attack until it is too late. Substations are therefore shut off and do not respond to commands to come back online. Accordingly, the system operator in the control center observes normal operating conditions while customers have no electricity.

In this type of attack, the antenna signal can be authenticated successfully using the method described in Section III-C. In the next step, to defend against the attack, our methodology infers substation measurements and control actions from the magnetic field signal and compares the results with the SCADA network traffic to identify the malicious activities in the substation. In this step, the RF signal will show the circuit breaker opening action while there is no circuit breaker operation report in the SCADA system. Therefore, the control center will be able to intervene before the attacker can impart long-term damage.

B. *Attacker Level 2*

This attacker can go one layer deeper and compromise both the SCADA and the LF magnetic field measurement systems

[1] Even if the GPS signal is considered untrusted, the attacker needs to spoof $\left\lfloor \frac{n}{2} \right\rfloor + 1$ of the receivers to cause a false negative in RFDIDS. Meanwhile, spoofed GPS signals cannot cause false positives.

simultaneously. Accordingly, in this type of attacker, we also cannot trust any data from the LF magnetic field measurement system. However, the lightning database and sferics data from other receivers are still trusted entities. Lightning database is formed by a network of LF receivers, and includes the location, occurrence time, and intensity of lightning strokes in each time instant. As it will be discussed in Section III-C, by extracting the sferics from the LF measurement signal and comparing them with the presumed arrival times based on current lightning locations, we can check the integrity of the antenna's signal in real time. Should the LF data fail the authentication test, the control center may intervene to prevent significant damage. After the validation of magnetic field signal, the rest of the algorithm is similar to the one that we used for attacker level 1. Note that in this case, the attacker needs to entirely compromise two air-gapped systems (i.e., SCADA and LF measurement systems) at the same time, which is an extremely hard task.

C. Attacker Level 3

This attacker can completely compromise the SCADA system, antenna measurement system, and global lightning database. Hence, the only trusted entity in the case of such attacker is the sferics data from other receivers located in nearby substations. In this situation, the only way to authenticate the antenna signal is to leverage the sferics data from other receivers using the method described in Section III-C. If the signal authentication test fails in the first step, an intrusion alarm will be set in the control center; otherwise, the SCADA system validation test will be executed to find any sign of intrusions in the SCADA system. It should be noted that the attacker would have to compromise three separate, air-gapped systems in this type of attack, and yet his malicious activities will be detected by RFDIDS.

D. Attacker Level 4

This attacker can compromise the SCADA system, antenna measurement system, lightning database, and a portion of the other RF receivers in nearby substations. As we will describe later in Section III-C, even in this situation, if only one LF receiver works correctly, it will cause inconsistency in the lightning authentication scheme, illustrating a sign of an attack. The attacker compromising three air-gapped systems plus additional receivers' signals in nearby substations is an unlikely scenario, if not impossible.

III. Background

A. Power Grid Overview

The power grid is defined as an interconnected electricity network which aims to deliver electricity from producers to consumers [37]. A system-level view of a power grid and its different sectors are shown in Fig. 2. The grid consists of three main sectors, i.e., generation, transmission, and distribution, which are connected together through substations [3]. In the generation sector, much of the required energy is produced in large scale power plants at medium voltage (e.g., 13.8 kV). Then, the generated power is stepped up to a higher voltage (e.g., 345 kV) and is connected to the bulk power transmission network through substations to be transmitted over long distances. Finally, the electricity is stepped back down to the medium voltage level by substations as it nears consumers. The distribution sector feeds the consumers within a limited geographical area with medium voltage.

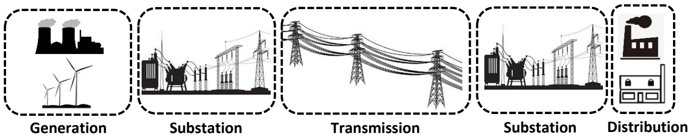


Fig. 2. The overall view of a power grid and its different sectors.

Inside the substations, there are measurement devices (e.g., current transformers (CTs) and voltage transformers (VTs)), which are responsible for measuring the electrical attributes of the substation circuits to monitor the condition of the whole substation. These measurements are polled periodically (every few seconds) in remote terminal units (RTUs) to be transmitted to the control center, where the goal is to monitor and control the entire power grid. The collection of RTUs from different substations along with the control center form a meshed communication network called SCADA system [38]. In the control center, energy management system (EMS) uses the gathered data to perform state estimation (SE). Doing so, the state variables (e.g., bus voltage magnitudes and their corresponding angles) of the power grid are calculated. The results of the SE are used in EMS applications such as system security assessment, optimal power flow (OPF), and reactive power control. EMS applications perform different calculations in order to specify control decisions to be implemented in the substations or power plants. The main control actions that can be implemented in power system substations are circuit switching (to change the topology of the grid) and transformer tap changing (to keep the system voltage level within its acceptable range). Since wide-area control of the power grid is based on remote measurements from substations, if the SCADA system is compromised by an attack, substations can be critically damaged. Alternatively, falsified data can trick the operator into making damaging erroneous changes, causing long-lasting widespread power blackouts.

Owing to the key role of substations in power systems, they have been a popular target for attackers to cause widespread blackouts [6], [39]. New technologies including microprocessor-based intelligent electronic devices (IEDs) and standardized networking protocols (e.g., TCP/IP) over wide area networks (WANs) are widely adopted in the substations. Remote access to IEDs or user interfaces in a substation for maintenance purposes is common. Further, there are many potential system vulnerabilities in substation components, e.g., unsecured standard protocols, remotely controllable IEDs, and unauthorized remote access to substation IEDs [40]–[44]. In addition, some substation IEDs have web servers which open them up to malicious remote configuration changes. The fact is, the power grid has a vast attack surface with many components that are insecure. Thus, it is critical that we provide novel ways to protect this vital system.

It is worth mentioning that even if firewalls and cryptography schemes are used for cybersecurity, weak security key management cryptography and misconfigured firewalls are still exposed to intruders. From the IT point of view, cybersecurity

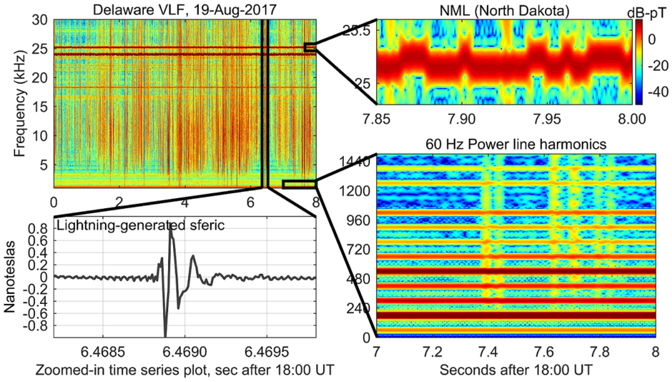


Fig. 3. Sample of an LF radio signal and its different components.

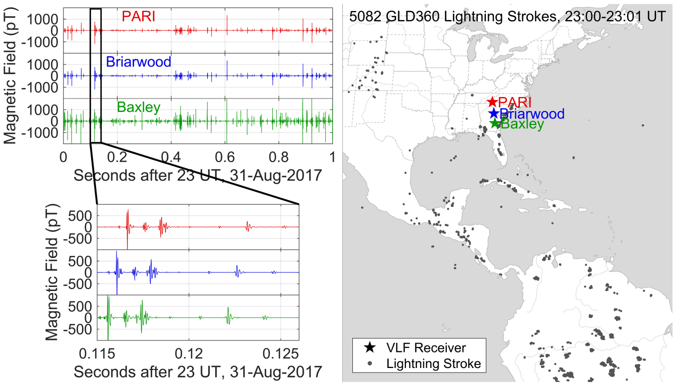


Fig. 4. Lightning impulses (sferics) at multiple LF radio receivers.

issues are well known and new security technologies are available. However, security research on the integration of IT and physical power systems, as an important critical infrastructure, is still an emerging area.

B. Radio Frequency (RF) Measurements and AWESOME Receiver

RF measurement of the magnetic field refers to capturing the magnetic field oscillations in the frequency range of <300 GHz [45]. Since the fundamental frequency of the power grid is 60 Hz, in our proposed method, we focused on the LF range (<100 kHz) signals, which are within the range of the RF emissions generated directly by power lines. The LF radio receiver to collect the magnetic field emissions, known as atmospheric weather electromagnetic system for observation, modeling, and education (AWESOME) [46], was completed in 2010 and then upgraded in 2015. The distinguishing features of this receiver are extremely good sensitivity, frequency and phase response, timing accuracy, and dynamic range. Accordingly, we used this receiver in our method to capture the magnetic fields of substation circuits. The detailed explanation about AWESOME receiver can be found in [46].

An example of LF radio data recorded by AWESOME receiver is shown in Fig. 3. These data are taken from a receiver in Dover, Delaware, recording magnetic field as a function of time. The top left panel shows a spectrogram of the data, with horizontal axis in seconds, vertical axis in frequency, and color indicating the strength of each frequency at each time instant. The horizontal lines in the top left spectrogram are radio stations used by the US Navy for submarine communications. A zoom-in in the top right panel shows one in particular known as NML, at 25.2 kHz, which broadcast from North Dakota, very far away from the receiver. The vertical lines in the spectrogram show radio atmospherics, or ‘sferics’. These may originate from lightning strokes many thousands of miles away, so could be from almost anywhere around the world. Since a lightning flash occurs roughly 40 times per second on average, and the sferic travels to global distance, there are numerous sferics in the data, as is clearly evident in this example. The arrival times and amplitudes of the sferics are determined by the quasi-random distribution of global lightning at that moment. One selected sferic is shown in the lower left thumbnail. The characteristics of this sferic are complex and depend on the type of lightning, the distance from the lightning stroke to the receiver, and the propagation conditions in the upper atmosphere. As such, each sferic looks unique. Roughly speaking, this is a random natural phenomenon. Indeed, it is almost impossible to get a similar lightning signals in two different time instants. Technically a lightning sferic lasts roughly 1 ms. If there is exactly 1 sferic randomly inserted each second, and conservatively assuming we have only 1 ms arrival time accuracy then, the probability of two 1-second segments having the same impulse location would therefore be 1/1000. In practice, we have many sferics per second which reduces this probability to be exceedingly small. The interesting point is that the AWESOME receiver can detect sferics regardless of weather conditions. The bottom right panel of Fig. 3 shows the harmonics of 60 Hz observed in the receiver. This particular receiver is located at an educational museum not near a substation, and yet many harmonics of 60 Hz are clearly detected due to the high sensitivity of the receiver.

C. Lightning Watermark and Global Lightning Detection Database

A critical differentiator of our approach is a novel scheme to authenticate the measured RF signal. While many smart grid cybersecurity efforts involve setting up a new sensor, they all share the same issue that if a capable hacker gains access to the SCADA system, all these sensor data can be faked. However, our LF data diagnostic does not suffer from this limitation, and thus, is more secure against spoofing/replay attacks.

Typical LF data contains not only the power line harmonic radiation and impulses, but also the sferics from global lightning strokes as described in Section III-B. An example of LF data detected at multiple sites is shown in Fig. 4. The top three panels show magnetic field signatures in a single second at three sites in Georgia, USA. The bottom three panels show a close-up of a 12-ms segment. There are a huge number of impulsive sferics from lightning all over the world at any time, many of which are detected by GLD360 (i.e., a network of RF receivers to detect lightning strokes around the globe), as shown in the map on the right. As an interesting observation, this quasi-random distribution of impulses acts as a watermark/nonce.

With the knowledge of lightning times and locations detected by GLD360, one could easily check that the impulse arrival times are consistent with the global constellation of

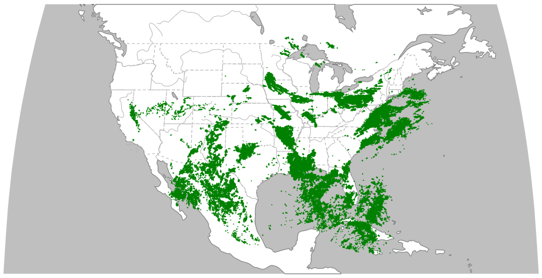


Fig. 5. Lightning locations within the continental USA on 19-Aug. 2017.

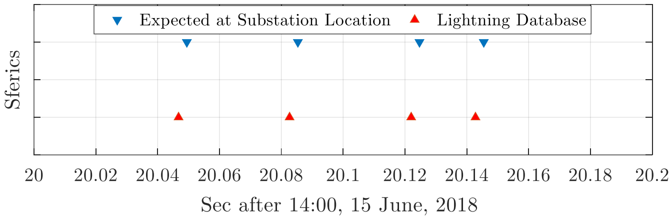
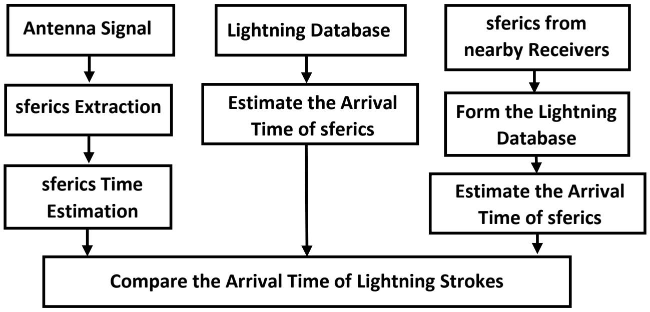


Fig. 6. The occurrence time of lightning strokes and their corresponding expected arrival time to the substation location (located in Midtown Atlanta).



Antenna Signal
Lightning Database
sferics from nearby Receivers
sferics Extraction
Estimate the Arrival Time of sferics
Form the Lightning Database
sferics Time Estimation
Estimate the Arrival Time of sferics
Compare the Arrival Time of Lightning Strokes

Fig. 7. The general structure of the lightning authentication scheme.

lightning, by simply accounting for propagation delays around the world at close to the speed of light, calculating the expected arrival times of sferics, and then verifying that impulses do indeed appear, thus authenticating the data.

Interestingly, however, even if perfect knowledge of global lightning activity did in fact exist and were available to a hacker, it would still be extremely difficult, if not impossible, to synthesize LF data. As the shape of a sferic evolves with distance and as a function of time of day, season, and other factors, synthesizing accurate LF data would require computationally intense physical models of propagation between the Earth and ionosphere that cannot be run anywhere near real time [47]. As such, the quasi-random distribution of global lightning makes for a one-way function that allows easy authentication but is practically impossible to synthesize. We will later discuss in Section VI-A3 that only replay attack is possible (not feasible) to be implemented on RFDIDS.

The lightning data are available from the Global Lightning Detection 360 (GLD360) network, which provides precise time (μs accuracy), location (km accuracy), and intensity of the vast majority ($\sim$80%) of lightning strokes around the globe. GLD360 uses an earlier version of the AWESOME receiver, licensed to a company called Vaisala [48]. Fig. 5 shows an example of lightning locations within the continental USA on 19-Aug. 2017. Using this precise database of lightning locations and times, it is straightforward to predict arrival times of impulsive sferics that should be seen by an LF receiver at any location. In fact, by having the GPS coordinates of the lightning strokes and the substation, we can calculate how long it takes a lightning signal to travel to the substation location. The accuracy of this prediction depends on the time accuracy of the GPS signal ($< 1\mu$s). As an example, Fig. 6 shows the occurrence time of lightning strokes and their corresponding expected arrival time to a substation located in Atlanta, GA, USA within a 200 ms time window. In this paper, we use the national lightning detection network (NLDN) database, which has the functionality similar to GLD360. However, NLDN captures the lightning sferics in the continental USA and is more precise than GLD360, meaning that in a constant time window, NLDN can capture more sferics than GLD360.

The general structure of the lightning authentication scheme is shown in Fig. 7. As can be seen, this scheme has three inputs: i) LF antenna signal which includes the magnetic field of the substation circuit, ii) lightning database which is acquired from a network of RF receivers, and iii) the detected sferics from the receivers located in nearby (e.g., <100 km) substations. The lightning authentication scheme leverages the correlation between these three inputs to identify any attacks on any one of them. The algorithm extracts the sferics from the first input by removing the signal caused by power line current, as formulated in (1) [49]. The resulting signal consists of a small noise with some impulses (sferics) (see top left corner in Fig. 4). We can define a threshold to detect the time of these sferics and identify their occurrence time.

$$B_{sferics}(t) = B(t) - B_{power}(t), \tag{1}$$

where $B(t)$ is the measured magnetic field signal (first input), and $Bpower(t)$ is the magnetic field signal caused by power line current which can be determined by a mathematical process expressed in Section IV.

The second input (i.e., lightning database) has three attributes including lightning location, its occurrence time, and its current intensity. Given the location of a lightning strike and a substation, also occurrence time of that lightning, we can easily calculate the expected arrival time of sferics at the substation location. The reason is that the impulsive electromagnetic signals from the lightning strokes travel at the speed of light in vacuum. The bottom left corner of Fig. 4 illustrates the sferics detected from three receivers at different locations. As can be seen, the sferics have the same shape with various detection time which results from their different distances from the lightning locations.

To improve the security of the lightning authentication method, we used the third input which is sferics from nearby substations. Since each utility owns a large number of substations (e.g., 50), this input can be used to form a secondary lightning database. To explain in more details, the time and location of the lightning strokes can be determined by three receivers forming a triangle. Suppose that our algorithm gets the sferics arrival time from three different substations (i.e., t_1, t_2, and t_3) as shown in Fig. 8. In this figure, t_0, x_0, and y_0 are three parameters which identify the lightning occurrence time

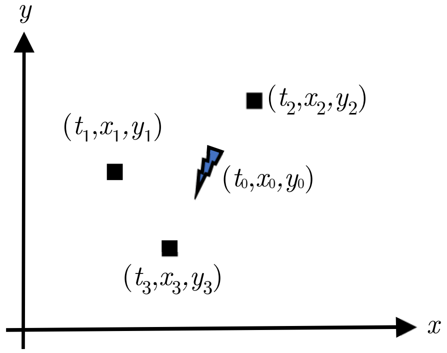


Fig. 8. Three different substations with LF receivers and a lightning strike between them.

and its location. For t_1, one can write the following equation:

$$t_1 = t_0 + \frac{\sqrt{(x_1 - x_0)^2 + (y_1 - y_0)^2}}{c}, \tag{2}$$

where c is the speed of light in vacuum. This equation means that the arrival time of a lightning sferic to a substation is a function of its occurrence time and the distance between the lightning location and the substation. By writing two other equations for t_2 and t_3 similarly, we will have three independent equations with three variables (i.e., t_0, x_0, and y_0). Solving this system of equations will form the secondary lightning database with lightning locations and occurrence time. Similar to the second input, this new database can be used to authenticate the first input signal.

Considering the above mentioned inputs in each substation, we can obtain three sequence of sferics within the specified time window. Any inconsistency between the arrival time of the sferics in these three inputs will likely be a sign of intrusion. Axiomatically, the existence of the third input increases the reliability of the RFDIDS by improving its data redundancy. In fact, even if the attacker can compromise the lightning database (second input) or it is not available at all, our method can still reliably authenticate the receiver's signal via the third input. In this condition, at least three other receivers from nearby substations are needed. In the other case, if only one substation deploys the receiver, the lightning database (the second input) can be leveraged to authenticate the measured LF signal.

IV. Radio Frequency (RF) Measurements in Power System Substations

As mentioned in Section I-C, at least four types of diagnostics can be extracted from the measured magnetic field signal: current signal harmonic content, power system fundamental frequency, impulses from sudden changes in the current signal, and sferics. The method for obtaining the last attribute (i.e., sferics) was explained in Section III-C. In the following sections, we will explain how we can extract the other three attributes. To do so, first, we need to find the relationship between the current flowing through a three-phase circuit and the corresponding measured magnetic field by our receiver. Technically, the magnetic field emission from a current density in the three-dimensional space can be calculated from the magnetic retarded vector potential. To explain in the mathematical format, the magnetic retarded vector potential, $\overrightarrow{A}$, for a given point source in the space can be calculated as [47]:

$$\vec{A}(\vec{r}) = \frac{\mu_0}{4\pi} \overrightarrow{I_i} \frac{e^{-jk|\vec{r}-\overrightarrow{r_i}|}}{|\vec{r}-\overrightarrow{r_i}|}, \tag{3}$$

where $\overrightarrow{I_i}$ and $\overrightarrow{r_i}$ are the current (as a phasor) and location of the i^{th} point source, respectively, with respect to the origin, k is the free space wavenumber, and $\overrightarrow{r}$ is the location of the receiver (i.e., the location where the magnetic field of the source point is measured). It should be noted that the free space wavenumber can be calculated as $k = 2\pi f/c$, where f denotes the frequency of the current flowing in the source point. Considering the fact that one can split each power line to small pieces of source points, the total magnetic retarded vector potential from the source points can be written as:

$$\vec{A}(\vec{r}) = \frac{\mu_0}{4\pi} \sum_i \overrightarrow{I_i} \frac{e^{-jk|\vec{r}-\overrightarrow{r_i}|}}{|\vec{r}-\overrightarrow{r_i}|}. \tag{4}$$

In addition, the method of images is used to account for the ground plane, allowing the entire problem to be treated as homogeneous free space. Therefore, every current element is accompanied by an image current, at the opposite location on the other side of the ground plane, with horizontal current magnitude in the opposite direction. All things considered, the magnetic field at a given location (i.e., $\overrightarrow{B}(\overrightarrow{r})$) can be calculated through (5).

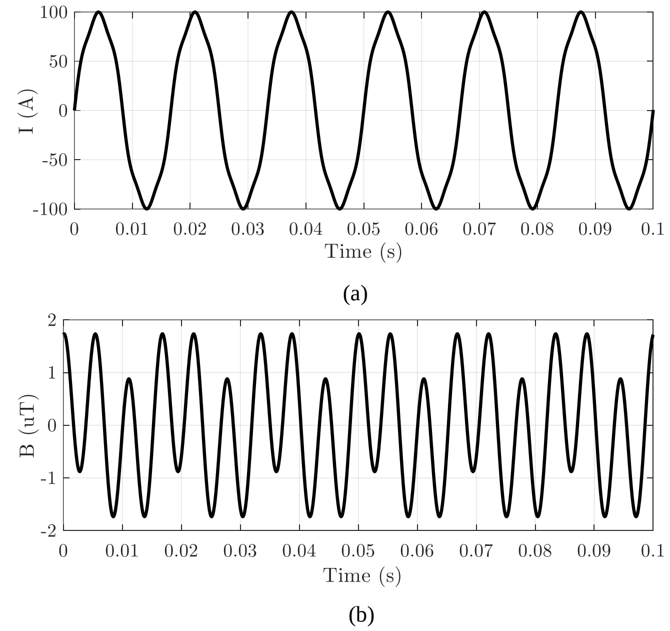
$$\overrightarrow{B}(\overrightarrow{r}) = \nabla \times \overrightarrow{A}(\overrightarrow{r}), \tag{5}$$

where ∇ is the curl operation on the given vector. Assuming the balanced three-phase condition in the circuit, one can calculate the magnetic field resulting from the three lines of the circuit in terms of the current flowing in one of the phases. Accordingly, in a fixed location for the receiver, the magnetic field of a three-phase line in each frequency can be expressed as follows:

$$B_f(I_f) = K_f I_f, \tag{6}$$

where B_f, K_f, and I_f denote magnetic field, constant coefficient, and current amplitude of the circuit at a certain frequency (f), respectively. Therefore, by analyzing the magnetic field measurements at each frequency, one can simply estimate the features of the circuit current (i.e., harmonic content, fundamental frequency, and impulses). Fig. 9 illustrates the current signal of a typical three-phase circuit and its corresponding magnetic field which can be seen from a 4 m distance below the circuit in the ground. Although the shapes of the waveforms look totally different, they have relatively definable relationship. The reason for this difference is that K_f is not the same in different frequencies. For this specific example, $K_f = 5.89 \times 10^{-9}$ for all of the harmonics except those of multiples of three (e.g., 60×6 Hz). In the case that the current has a harmonic of a multiple of three, $K_f = 2.88 \times 10^{-7}$. In practice, we can calculate K_f in the location of our receiver inside the substation and hence, by measuring the magnetic field of the substation circuits, we can reconstruct the current signal of different circuits.

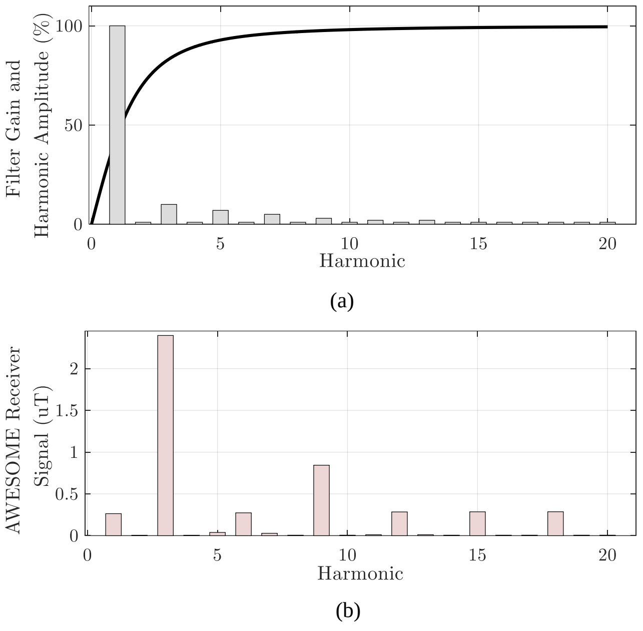
Note that the magnetic field signal that can be seen by the AWESOME receiver is slightly different than what is shown



(a)

(b)

Fig. 9. Typical waveform of: (a) Line current of a three-phase circuit, (b) Corresponding magnetic field.



(a)

(b)

Fig. 10. Illustration of: (a) Harmonic content of a typical circuit current and AWESOME receiver filter response (100 A = 100%), (b) Harmonic content of the corresponding receiver signal.

in Fig. 9, because this receiver has an inherent high pass filter inside that which further affects the measured signal. To explain in more details, Fig. 10 depicts the harmonic content of typical three-phase circuit current. The black solid line shows the frequency response of the AWESOME receiver filter. Finally, the harmonic content of the measured magnetic field signal by AWESOME receiver is illustrated in Fig. 10(b). Since we already know the behavior of the receiver's filter and the value of K_f in different frequencies, by analyzing the harmonic contents of the LF signal, we can estimate the useful information about the actual current signal of the substation circuits, which are leveraged in the proposed IDS.

A. Harmonic Content and Fundamental Frequency of the RF Signal

The aim of this section is to present the mathematical method for estimating the harmonic content and fundamental frequency of the measured magnetic field signal. As shown earlier in Section IV, the magnetic field signal is a periodical one with different harmonics. Accordingly, the general form of the antenna signal ($B(t)$) can be represented as follows:

$$B\left(t\right) = B_0 + \sum_{n=1}^{m} B_n \sin\left(n\omega_0 t + \phi_n\right), \tag{7}$$

where B_n and ϕ_n denote the amplitude and phase of the n^{th} harmonic, respectively. Also, ω_0 stands for the fundamental angular frequency and can be defined as $\omega_0 = 2\pi f_0$. Finally, B_0 is the DC component of the receiver's signal. In (7), there are $2m+2$ variables (i.e., $B_0, ..., B_m$, $\phi_1, ..., \phi_m$, and f_0) which should be determined by our algorithm. In this paper, we use the nonlinear least-square algorithm to estimate the aforementioned parameters of the antenna signal [50]. This algorithm finds the best fit of the measured signal to the specified mathematical form of that (i.e., (7)). Suppose that we have a data window with $N > 2m+2$ samples. Therefore, for k^{th} data sample, we can write the following equation:

$$B\left[k\right] = B_0 + \sum_{n=1}^{m} B_n \sin\left(n\omega_0 \Delta T k + \phi_n\right), \qquad \forall k = 0, 1, .., N-1 \tag{8}$$

where ΔT denotes the sampling time period. Now, let's define $\boldsymbol{x}$ and $\boldsymbol{B}$ as the vector of variables and data samples, and f as the function which represents the right hand side of (8). The dimensions of $\boldsymbol{x}$ and $\boldsymbol{B}$ are $(2m+2) \times 1$ and $N \times 1$, respectively. Accordingly, we can rewrite (8) as:

$$\boldsymbol{B} = f(\boldsymbol{x}). \tag{9}$$

With some mathematical manipulations [50], it can be proven that we can estimate the value of $\boldsymbol{x}$ iteratively as:

$$\boldsymbol{x}_{i+1} = \boldsymbol{x}_i + \left(f'^T(\boldsymbol{x}_i) f'(\boldsymbol{x}_i)\right)^{-1} f'^T(\boldsymbol{x}_i)(\boldsymbol{B} - f(\boldsymbol{x}_i)), \tag{10}$$

where $f'(\boldsymbol{x})$ stands for the first derivative of f with respect to $\boldsymbol{x}$. We continue this process until we get to the convergence point, that is:

$$|\boldsymbol{x}_{i+1} - \boldsymbol{x}_i| < \varepsilon \tag{11}$$

B. Impulses in the RF Signal

The aim of this section is to extract the impulses from the receiver's signal. These impulses stem from either the circuit breaker switching actions or lightning strokes. However, there are distinguishing features that allows us to differentiate between the impulses from lightning strokes and circuit breaker operation. The main difference is that the circuit breaker operation impulse is always accompanied by a sudden drop/increase of the first harmonic (e.g. 60 Hz) in the circuit current, and hence, the magnetic field emission from that circuit. Moreover,

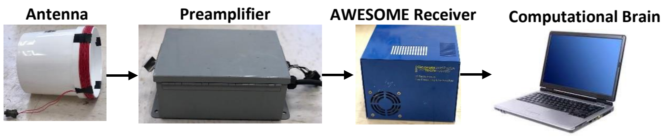


Fig. 11. Different components of the measurement setup.

the resulting impulse from a circuit switching causes higher electromagnetic overshoot than that of a lightning sferic. In this paper, we used the equation stated in (1) to extract the impulses from magnetic field signal.

V. Numerical Validation and Case Studies

A. Measurement Setup

In order to have comprehensive analysis, we will present a set of experimental results as well as simulation ones in the following sections. The experimental results come from the measurements inside multiple power substations. The first two substations are owned by Choptank Electric, A Touchstone Energy Cooperative, which is a not-for-profit, member-owned, electric distribution Co-op serving approximately 54,000 residential, commercial, and industrial members in all 9 counties on Marylands Eastern Shore (over 6,264 miles) [51]. Another substation is located in an urban area in Atlanta, Georgia, USA and is owned by Georgia Power, which is the largest utility that is operated by Southern Company. Georgia Power is an investor-owned, tax-paying public utility that serves more than 2.4 million customers in 155 counties of Georgia [52]. We have built an LF antenna, which consists of 20 AWG copper wire wrapped around a 23-cm-diameter circle in 42 turns, to capture the magnetic field emissions from these substations. In order to gain a good signal quality, have the impedance matching, and capture a suitable bandwidth, we designed the antenna such that its resistance and inductance are 1.0 Ω and 1.0 mH, respectively. The antenna placed right below the AC circuits on the ground with 10 ft distance, such that its surface is perpendicular to the circuit current. The general view of the measurement setup is shown in Fig. 11. In our setup, we used 1 MHz as a sampling frequency for capturing the LF data. In some cases, we did not have access to experimental results because of the attacks considerable economic consequences (several million dollars). In such cases, we illustrated the RFDIDS's performance through simulation results. In the simulations, we considered worst case operating conditions and scenarios to assure the promising performance of RFDIDS. For instance, to model the measurement noise, %10 (or 20 dB SNR) Gaussian noise is superimposed onto the magnetic field measurement signal [53], [54].

B. Attack Scenarios on Substations

The air-gapped IDS described above can be applied in a variety of situations to secure power system substations against cyberattacks. Some important applications of our method are explained in the following subsections. Note that the applicability of the proposed structure is not limited to the mentioned cases. In fact, any attack that changes the current waveform of a power circuit has the potential to be detected by RFDIDS.

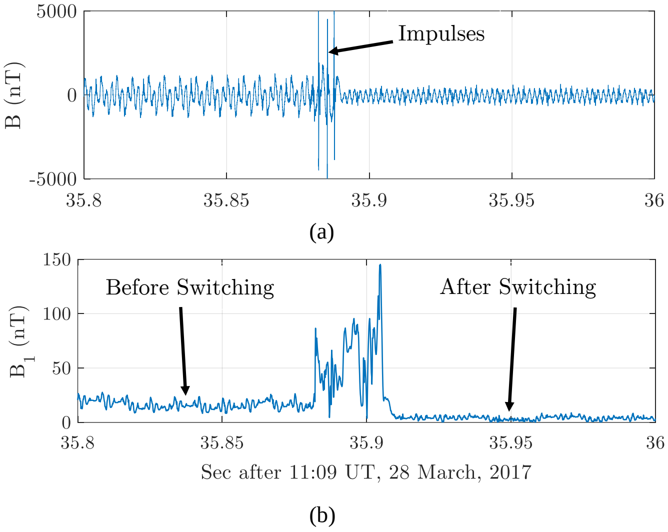
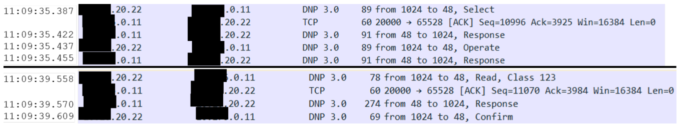


Fig. 12. Measured magnetic field in a real-world substation during a circuit breaker opening event: (a) Magnetic field, (b) 60 Hz component of the magnetic field.

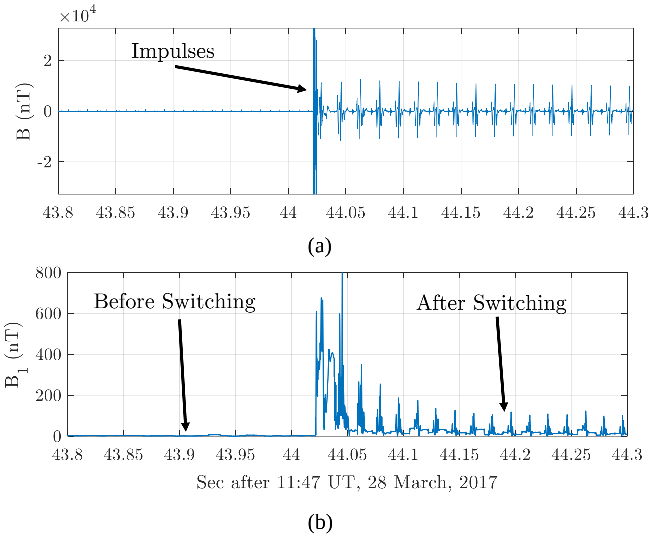


```
11:09:35.387 [redacted].20.22   [redacted].0.11    DNP 3.0   89 from 1024 to 48, Select
             [redacted].0.11    [redacted].20.22   TCP       60 20000 → 65528 [ACK] Seq=10996 Ack=3925 Win=16384 Len=0
11:09:35.422 [redacted].0.11    [redacted].20.22   DNP 3.0   91 from 48 to 1024, Response
11:09:35.437 [redacted].20.22   [redacted].0.11    DNP 3.0   89 from 1024 to 48, Operate
11:09:35.455 [redacted].0.11    [redacted].20.22   DNP 3.0   91 from 48 to 1024, Response
11:09:39.558 [redacted].20.22   [redacted].0.11    DNP 3.0   78 from 1024 to 48, Read, Class 123
             [redacted].0.11    [redacted].20.22   TCP       60 20000 → 65528 [ACK] Seq=11070 Ack=3984 Win=16384 Len=0
11:09:39.570 [redacted].0.11    [redacted].20.22   DNP 3.0  274 from 48 to 1024, Response
11:09:39.609 [redacted].20.22   [redacted].0.11    DNP 3.0   69 from 1024 to 48, Confirm
```

Fig. 13. Network traffic associated with the circuit breaker opening event.

1) Circuit Breaker Malicious Switching: The opening or closing of circuit breakers by an attacker can lead to large-scale power outages such as the Ukrainian power grid blackouts in 2015 and 2016 [4]–[6]. The circuit breaker operation is accompanied by a sudden decrease/increase in the line current. This generates a radiated magnetic field impulse along with a reduced/increased 60 Hz magnetic field around the power line. Accordingly, the impulsive signals and amplitude of the 60 Hz component of the magnetic field are two diagnostic tools that are leveraged for detecting switching events. Note that these two conditions should occur at the same time to represent the circuit switching event as there are other normal conditions which can cause one of the aforementioned situations. For example, in the case of load increase/decrease, the amplitude of the 60 Hz component will increase/decrease without the presence of any impulses. Also, the presence of impulse without the change in the 60 Hz component implies the lightning sferics.

To evaluate the developed theory, we recorded the magnetic field of substation circuits during several switching events using our measurement setup. Since planned switching actions rarely (e.g., every six months for maintenance purposes) occur in power substations, we only had a chance to record the magnetic field of substation circuits during several (i.e., three opening and three closing) switching actions in three substations mentioned in Section V-A. From the multiple switching incidents, two general cases are chosen to be illustrated in this section. However, the following explanations hold true for all of the recorded cases. Fig. 12 illustrates the magnetic field signal and its 60 Hz component as a function of time. As can be seen, the circuit breaker opening occurs at 11:09:35 since there



(a)

(b)

Fig. 14. Measured magnetic field in a real-world substation during a circuit breaker closing event: (a) Magnetic field, (b) 60 Hz component of the magnetic field.

are three impulse signals (corresponding to three phases of the circuit breaker) with reduced 60 Hz magnetic field (drops to zero) after the circuit transient. Because this event was a legitimate circuit breaker operation, the magnetic field signal is consistent with the network traffic which is shown in Fig. 13. According to this figure, the trip command is sent to the the circuit breaker at 11:09:35 utilizing the *Select then Operate* function code in DNP 3.0 protocol. Four seconds after the operation of the circuit breaker, the master controller reads the status of the breaker to make sure the trip command has been implemented successfully. In the case of an attack, we will see the normal operating condition (no sign of switching) in the network traffic as the attacker tries to hide his malicious activity. In contrast to the circuit opening event, Fig. 14 shows the magnetic field signal and its 60 Hz component as a function of time during a circuit closing incident. The impulses along with the increase in the 60 Hz harmonic (suddenly increases from zero) at 11:47:44 implies a circuit breaker closing event.

2) Transformer Malicious Tap Changing: A transformer is a critical and expensive piece of equipment in power system substations that transfers electrical power between two circuits through electromagnetic induction. Transformers are used to increase or decrease the voltage levels in power grids. Distribution substations are usually equipped with on load tap changers (OLTCs). OLTCs help transformers hold the secondary voltage level in the nominal value regardless of load current. Although transformers have not been a direct target of cyberattacks so far, we will show in the following paragraph that if an attacker gets access to the substation network, he will be able to cause significant damage to them. Recovering from such an attack needs a significant amount of time. For example, a physical attack on a substation in California on April 16, 2013 resulted in damage to 17 giant transformers and 27 days of repair time [55]. This attack resulted in over 15 million USD worth of damage.

If a hacker gets access to the controller of the transformer OLTC, he can cause substantial damage to the substation. Let us assume that hackers have gained full control of a substation. Assuming the typical configuration of two parallel transformers in power substations, the attacker could change the OLTC setting of one transformer. Meanwhile, they can send the spoofed current and temperature readings so that the utility does not detect the wrong OLTC settings. An incorrect OLTC setting can result in circulating current flowing through the parallel transformers, which increases losses in power transformers. The increased load leads to overheating of the affected transformers, which contain thousands of liters of oil. The rising oil temperature deteriorates the dielectric properties and results in an electrical breakdown, and the transformer can catch fire. The substation may be completely destroyed and the fire may spread to nearby neighborhoods. Recovering from such an event may take weeks or months. In fact, The substation will require substantial refurbishment including decontamination of the soil, rebuilding the foundation and grounding system, acquisition and installation of a replacement transformer as well as all other primary and secondary equipment affected by the fire. This attack can also occur in bulk transformers, which have been identified as a major vulnerability of power grids. Incorrect tap changing transformer operation can even lead to voltage problems and voltage collapse.

This stealth attack takes 10s of minutes to reach a catastrophic state, whereas RFDIDS can detect the problem within seconds. Our algorithm is able to estimate the flowing current in power circuits within an acceptable level of error. By monitoring the amplitude of the 60 Hz component of the transformer current, we can detect such attacks and prevent widespread damage to the substation transformer. To further illustrate this attack with simulation results, let's consider a simple substation configuration with two identical parallel transformers supplying a single distribution feeder with a constant current load ($I_{load} = 1$ p.u.), Fig. 15. In normal conditions, each transformer supplies half the feeders load. In this figure, V_{th} and Z_{th} represent the voltage and impedance of the Thevenin equivalent circuit of the transmission system, respectively. Assume that the attacker alters the tap changer settings of T_1 ($\varepsilon_1 = 0.1$) and T_2 ($\varepsilon_2 = 0$). In this circumstance, considering typical values $V_2 = 1$ p.u., $n = 1$, and $X = X_1 = X_2 = 0.01$ p.u., we can write the following equations:

$$V_1 = \frac{V_2}{(n\,(1+\varepsilon_1))} + I_1 \times jX_1, \tag{12}$$

$$V_1 = \frac{V_2}{(n\,(1+\varepsilon_2))} + I_2 \times jX_2. \tag{13}$$

With some mathematical manipulations, we can omit V_1 from (12) and (13) and write the relation between I_1 and I_2 as:

$$I_1 - I_2 = \frac{V_2}{jX}\left(\frac{1}{n\,(1+\varepsilon_2)} - \frac{1}{n\,(1+\varepsilon_1)}\right). \tag{14}$$

On the other hand, we know that the summation of transformer currents equals the load current:

$$\frac{I_1}{n\,(1+\varepsilon_1)} + \frac{I_2}{n\,(1+\varepsilon_2)} = I_{load}. \tag{15}$$

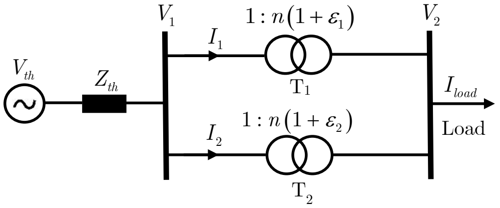


Fig. 15. Substation configuration with two identical parallel transformers.

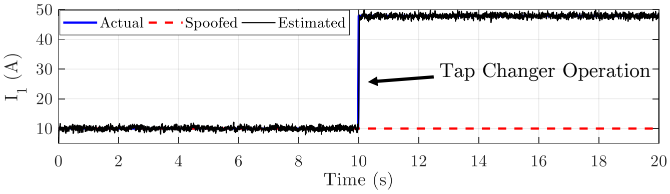


Fig. 16. Illustration of malicious tap changing attack on a power transformer and its detection by RFDIDS.

Given the typical parameters in this example, the set of linear equations (14)–(15) is solved and the transformer currents are calculated as $I_1 = 4.790\angle - 83.7°$ p.u. and $I_2 = 4.360\angle 83.1°$ p.u. Notice that $|I_1|$ and $|I_2|$ are much larger than $|I_{load}|$. The physical interpretation is that there is a large component of the current that circulates from one transformer to the other without entering the load. This circulating current serves no useful purpose. In fact, it is harmful, wasting energy and possibly overheating the transformers. Another subtle point is that even if the load current is zero ($I_{load} = 0$), we still get a large circulating current [56].

We simulated the previously described scenario in which the malicious tap changer operation by the attacker causes a significant circulating current in both of the transformers. Fig. 16 shows the amplitudes of the actual, spoofed, and estimated currents associated with the first transformer (T_1). To consider the worst case measurement scenario, we added 20 dB noise to the measured signal. As shown in the figure, RFDIDS can successfully track the current change in the transformer and detect the malicious tap changing attack on that in the presence of 20 dB measurement noise.

3) False Data Injection to Substation RTUs: This is one of the most common cyberattacks in power system substations. In this attack, the attacker tries to manipulate the information in RTUs and report false data to the control center. As mentioned in Section IV-A, our proposed algorithm is able to estimate the amplitude and fundamental frequency of the circuit current with a reasonable error. Since the values of these two variables are periodically reported to the control center, our algorithm can check the reported values and compare with the values obtained from the RF receiver to detect any false data injection attack. In the case of attack, we will see a considerable difference between the reported value of the parameters and their estimated values from RF measurements.

To show the effectiveness of the RFDIDS in this type of attack, we recorded the magnetic field of a substation circuit as a function of time during a switching event. The goal is to estimate the circuit current before and after the switching event and compare it with the output of direct measurement devices in the SCADA system. To evaluate the proposed algorithm in the worst case (in terms of noise), a substation is chosen which is located in a metropolitan area (i.e., Midtown) in Atlanta, GA, USA. Fig. 17 depicts the estimated amplitude of the circuit current before and after the switching incident. In this event, the other side of the circuit was opened at 13:42:36 through the operation of the circuit breaker while our side was still connected to the Midtown substation. In the estimation algorithm, we assumed that the circuit is operated in the balanced condition, meaning that all of the three phases has the same current amplitude with 120 degrees phase shift with respect to each other. According to Fig. 17, the estimation algorithm reveals the following values for the amplitude of the phase current before and after the switching incident, respectively: 175 A and 25 A. It should be noted that this 25 A is indeed the charging current of the circuit which is supplied by the substation.

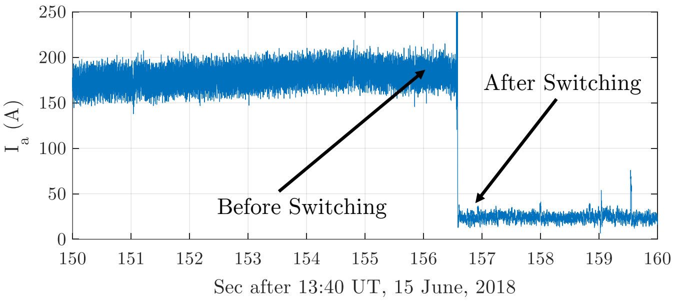


Fig. 17. Estimated amplitude of the circuit current from RF measurements during a circuit opening event.

The actual three phase current values before and after the switching event that are obtained from the SCADA system measurements, are summarized in Table I. As can be seen, the estimation error in such a noisy area is still reasonable and is almost 10% in the worst condition. Note that this error partially stems from the assumption of three phase balanced operation. By deploying three receivers, we can easily eliminate the error causing by unbalanced operation of the circuit. All things considered, it is obvious that RFDIDS can successfully detect any false data injection attack on the circuit current amplitude by defining a threshold of 12%. If there is a deviation greater than 12% between the reported value of the current and its estimated value, one can claim that it is a false data injection attack. This means that if the attacker spoofs the reported value of the current amplitude with less than 12%, the proposed method will return a false positive (normal operation) for that attack. However, such a small spoofing attack can hardly cause damage or erroneous decisions in the power grid.

Regarding the threshold for the frequency estimation algorithm, we did not have access to the value reported by the SCADA system to make a fair comparison. Instead, we performed an illustrative simulation, which will be discussed in Section VI-B2. According to our simulations, a suitable threshold for the system frequency is 0.05 Hz. By estimating the aforementioned attributes from RF measurements and considering the determined thresholds, we can detect false data injection attack to protective relays as well. We omitted the results associated with this attack due to the lack of space.

TABLE I. CURRENT AMPLITUDE OF THE CIRCUIT BEFORE AND AFTER THE CIRCUIT OPENING EVENT OBTAINED FROM SCADA MEASUREMENTS AND THE CORRESPONDING ESTIMATION ERROR OF RFDIDS

Phase	I_{pre}^{SCADA} (A)	Error(%)	I_{post}^{SCADA} (A)	Error(%)
A	174	0.57	26	3.84
B	182	3.84	27	7.40
C	158	10.75	24	4.16

VI. ROBUSTNESS AND RESILIENCY OF RFDIDS

Our proposed algorithm has two general stages: i) magnetic field validation (lightning authentication) stage, and ii) measurement and command validation stage. The aim of this section is to discuss the robustness and resiliency of these two stages in different challenging situations.

A. Magnetic Field Validation (Lightning Authentication) Stage

In this stage, the integrity of the measured magnetic field signal is checked for any possible manipulations. According to Section III-C, the lightning authentication scheme can check the integrity of the measured signal by comparing the arrival time of the lightning sferics obtained from three different inputs: lightning database, secondary lightning database formed by the receivers at nearby substations, and the receiver in the current substation. The following challenges can be discussed for the algorithm of this stage.

1) The Length of Moving Time Window: As mentioned before, the lightning authentication scheme checks the signal's integrity in a moving time window. Here a fundamental question arises: what is the optimal length of this time window? There are two main challenges in answering this question. If the length of the time window is too short, there is a possibility that no lightning sferic is detected in some time windows, and thus, the authentication scheme becomes vulnerable or conservative (depending on the type of decision in the case of no lightning in the current data window). On the other hand, if the length of the data window is too long, the proposed IDS will experience too much delay in identifying the malicious activities in the substations. Accordingly, a reasonable trade-off should be made between the number of sferics in the current time window and the length of that. To determine this, we performed a statistical analysis on the recorded magnetic field signal from multiple substations as well as the lightning database. The analyzed data includes the signal of AWESOME receiver obtained from three substations and in two different seasons and hours (2 hours in total). Also, the lightning database of the corresponding days are analyzed for 24 hours. As shown in Fig. 18, two consecutive sferics can be detected by the AWESOME receiver and lightning database in a time window with the length of two seconds (with the probability of %99.99). Therefore, by considering a moving data window with the length of greater than two seconds, if the attacker feeds the algorithm with a spoofed signal without any sferics, he will succeed with the probability of 10^{-4}. In the case that he feeds the RFDIDS with sferics included signal, the successful rate is zero. Note that the brute force attacks cannot be implemented in power substations, as with the first sign of intrusion, the substation control changes to manual mode.

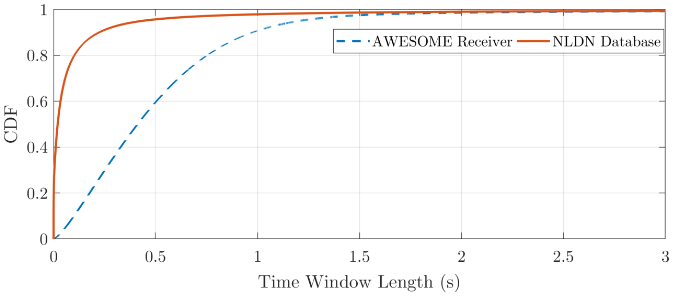


Fig. 18. Cumulative distribution function (CDF) of the appearance of two consecutive sferics in terms of time window length.

2) The Level of Consistency between the Inputs: Our statistical analysis (see Fig. 18) shows that a network of receivers can pickup a major portion of the lightning sferics in each time window while our fabricated receivers are able to pickup a subset of those sferics. With a similar reasoning, the probability that a sferic shows up in the secondary database formed by the network of receivers in nearby substations is more than that of a single receiver and less than that of the lightning database. The reason is that the number of receivers used in the lightning database is much higher than that of the secondary lightning database.

Fig. 19 shows the typical arrival time of lightning sferics obtained from: lightning database, secondary lightning database, and the receiver located in the current substation. In this specific time window, it is expected that four sferics are detected by the AWESOME receiver. Also, the secondary lightning database misses one of those sferics and detects the other three one. Finally, the AWESOME receiver detects two sferics. Considering this point, the proposed scheme compares the arrival time of the sferics from bottom to the top. This means that our method extracts the lightning sferics from the antenna signal, and then, sees that if all of these sferics are expected according to the primary and secondary lightning database. There is a possibility that a sferic is detected by the AWESOME receiver and its corresponding data does not exist in the primary and secondary lightning databases. Therefore, we need to define a suitable threshold for the number of inconsistencies in each time window. To find the appropriate threshold, we performed a statistical analysis on 1.5 hours of the recorded data with different data window lengths and thresholds. As shown in Table II, with the time window length of 4 seconds and the threshold of 3, we will have 99.99% true positive rate (normal conditions). By choosing the mentioned parameters as the settings of the lightning authentication method, we tested the proposed algorithm with another 30 minutes of LF signal that we did not consider in our statistical analysis. The result of this test is 100% true positive rate and 0% false negative rate. We also tested our algorithm with the determined parameters and by feeding it with a 15 minutes replayed (fake) signal. In this experiment, the true negative (attack) rate is acquired 99.99% and the false positive rate is obtained 0.01%, which show the effectiveness of RFDIDS in authenticating the LF signal. Fig. 20 depicts the extracted lightning sferics from the antenna signal during a switching event and the corresponding lightning database sferics. In this 10 seconds window, there is only one sferic in the receiver's signal that its corresponding sferic does not exist in the lightning database.

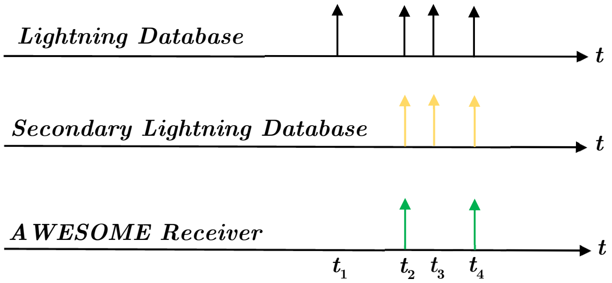


Fig. 19. A typical illustration of the arrival time of lightning sferics obtained from: lightning database, secondary lightning database, and the receiver located in the current substation (the order is from top to below).

TABLE II. STATISTICAL ANALYSIS OF THE LF SIGNAL

Win. Length (s)	Threshold (#)	True Pos. (%)	False Neg. (%)
3	0	51.65	48.35
	1	76.14	23.86
	2	87.29	12.71
	3	96.85	3.15
4	0	63.31	36.69
	1	82.58	17.42
	2	93.74	6.26
	3	99.99	0.01

3) Feasibility of Attacks: The difficulties associated with launching various levels of attacks on the lightning authentication scheme were mentioned in Section II. As discussed, the attacker needs to compromise all of the three inputs of the first stage algorithm to be able to circumvent the authentication scheme. However, even if the attacker can compromise all of the three stages, he still needs to synthesize the LF data to implement malicious activities in the substation. As the shape of a sferic evolves with distance and as a function of time of day, season, and other factors, synthesizing accurate LF data would require computationally intense physical models of propagation between the Earth and ionosphere that cannot be run in real time [47]. Indeed, the quasi-random distribution of global lightning makes a one-way function that allows easy authentication but is practically impossible to synthesize. In addition to this, to synthesize an accurate LF signal, the attacker needs to know the exact geographic distances between all of the substations in the system which is not easily accessible.

The only way to circumvent the first stage of RFDIDS is to launch a replay attack. This means that the attacker needs to record the signals of the three inputs and replay them to the proposed scheme. In order to successfully defeat the whole IDS, the attacker should also replay the relevant SCADA network traffic to the control center. Needles to say, recording and spoofing the mentioned four signals are extremely hard, if not impossible.

B. Measurement and Command Validation Stage

As mentioned earlier, this stage of the proposed algorithm is responsible for extracting the harmonic content, fundamental frequency, and impulses (caused by switching actions) of the measured magnetic field signal. According to (1), the accuracy of the impulse detection approach directly depends on the accuracy and robustness of the harmonic content and fundamental frequency estimation algorithms, which are analyzed in the following subsections. To test the proposed algorithm, we simulated a set of illustrative case studies which represent the worst case operation condition of power substations that can rarely occur in practice.

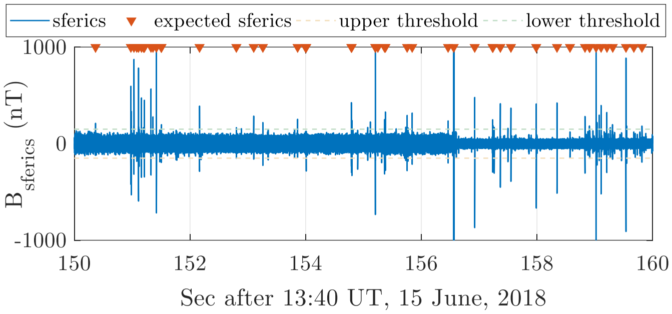


Fig. 20. The extracted lightning sferics from the antenna signal during the switching event and the corresponding expected sferics obtained from lightning database.

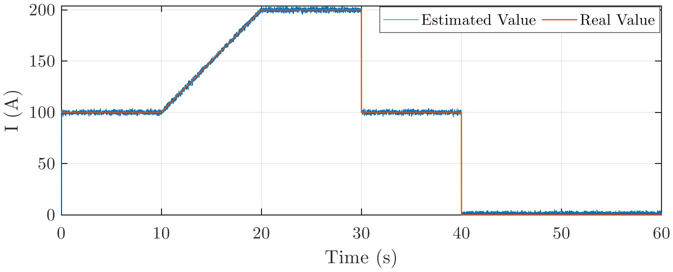


Fig. 21. Illustration of the robustness of the harmonic estimation algorithm in the presence of %10 noise.

1) Performance of the Harmonic Content Estimation Algorithm: To evaluate the performance of this algorithm, we simulated a signal representing the worst case operating conditions of power substations. The generated signal starts with a constant amplitude, then, increases with a ramp rate, and finally, suddenly decreases twice. Also, to model the measurement noise, %10 (or 20 dB SNR) Gaussian noise is superimposed onto the reference input signal [53], [54]. The general view of the test signal is shown in Fig. 21. Also, the actual and estimated amplitude of the signal's first harmonic is depicted in this figure with red and blue colors, respectively. A robust algorithm should be able to track the voltage amplitude of the circuit with negligible error. As can be seen in Fig. 21, the adopted algorithm is robust against noise and abnormal operating conditions even in the worst cases, which implies the practical merits of the proposed approach in real-world applications.

2) Performance of the Fundamental Frequency Estimation Algorithm: Similar to the previous section, we simulated a signal for the worst case operating condition associated with the system frequency. The generated signal starts with a constant frequency, and then, its frequency increases with a ramp rate. Also, to model the measurement noise, %10 (or 20 dB SNR) Gaussian noise is superimposed onto the reference input signal. Note that the fundamental frequency of the power system cannot change suddenly as it directly depends on the rotating speed of the synchronous generators [57]. The actual and estimated values of the system fundamental frequency is shown in Fig. 22. As can be seen, the frequency estimation algorithm

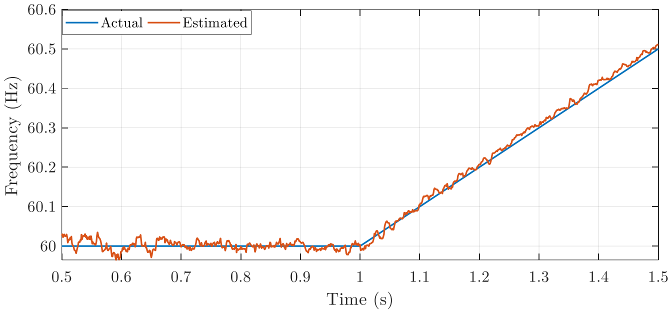


Fig. 22. Illustration of the robustness of the fundamental frequency estimation algorithm in the presence of 10% noise.

can successfully track the actual fundamental frequency of the magnetic field signal with negligible amount of error even in the worst condition.

VII. Conclusion and Possible Directions

Recent widespread blackouts throughout the world caused by cyberattacks have shed light on the fact that the electric power networks require reliable and robust defense mechanisms to prevent such attacks and reduce their damaging consequences. With this aim in mind, this paper proposed an air-gapped physical signal-based distributed intrusion detection system (i.e., RFDIDS) to protect power substations (as the most critical part of power networks) against advanced types of cyberattacks. Although in the proposed IDS, the SCADA system and even the side channel measurements are considered untrusted entities, it still can provide high level of security to protect substations against advanced types of attacks. In fact, the RF signal is encoded with the quasi-random sequence of lightning strokes around the globe, which acts as a watermark/nonce and this is an effective feature to authenticate the signal. Once the RF signal's integrity is verified, we can estimate the substation measurement and control actions from the magnetic field measurements with high accuracy. This allows us to check the integrity of the SCADA system traffic. The simulation and real-world experimental results revealed the effectiveness of RFDIDS in authenticating the magnetic field signal and estimating the SCADA system measurements and commands with an acceptable level of resiliency and robustness.

Despite the progress made in this paper, there are still a set of challenges in the proposed scheme. Our future studies will focus on the following existing issues:

- In the lightning authentication scheme, we used the location and occurrence time of lightning strokes as diagnostic tools. Future studies can include the shape and intensity of sferics in the authentication scheme with machine learning methods in order to increase the security of this approach.
- The proposed effort in this paper analyzed the utilization of RF receivers placed inside the substation fences. We noticed that some of the circuit current attributes can be detected from the receivers located at distant locations. One possible future study is to investigate and formulate the use of remote LF antennas to monitor the substation activities.
- In this paper, we assumed that there is one antenna for securing each of the substation circuits. Future studies can focus on finding the optimal number and location of LF receivers to reduce the implementation cost.
- Another existing challenge is the lack of secure wide-area monitoring system for the power grid. Owing to the fact that the current SCADA system is highly unreliable and vulnerable, one can study the use of proposed substation monitoring system to quickly detect and defend against system level attacks (on multiple substations at the same time).

Acknowledgment

The authors would like to sincerely thank Choptank Electric (in Maryland's Eastern shore) and Georgia Power (in Atlanta) for giving us the opportunity to capture real-world measurements from their power substations. NLDN data were provided by Vaisala Inc under a cooperative agreement with Georgia Tech.

References

[1] M. Eremia and M. Shahidehpour, *Handbook of electrical power system dynamics: modeling, stability, and control*. John Wiley & Sons, 2013.

[2] A. J. Wood and B. F. Wollenberg, *Power generation, operation, and control*. John Wiley & Sons, 2012.

[3] J. D. Glover, M. S. Sarma, and T. Overbye, *Power System Analysis & Design*. Cengage Learning, 2012.

[4] K. Zetter. (July 2018) Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. [Online]. Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[5] R. M. Lee, M. J. Assante, and T. Conway, "ICS defense use case: Analysis of the cyber attack on the Ukrainian power grid," *Electricity Information Sharing and Analysis Center, SANS ICS*, 2016.

[6] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. on Power Syst.*, vol. 32, no. 4, pp. 3317–3318, 2017.

[7] M. Kumar. (March 2018) Dragonfly 2.0: Hacking Group Infiltrated European and US Power Facilities. [Online]. Available: https://thehackernews.com/2017/09/dragonfly-energy-hacking.html

[8] J. Langill, "Defending against the Dragonfly cyber security attacks," *Belden, White Paper*, pp. 1–33, 2014.

[9] S. Tatum. (March 2018) US accuses Russia of cyberattacks on power grid. [Online]. Available: https://www.cnn.com/2018/03/15/politics/dhs-fbi-russia-power-grid/index.html

[10] (March 2018) US power grid needs defense against looming cyber attacks. [Online]. Available: http://thehill.com/opinion/energy-environment/379980-us-power-grid-needs-defense-against-looming-cyber-attacks

[11] C. Kube. (July 2018) Dem, GOP senators join to ask Trump to get tough on Russia cyber threat. [Online]. Available: https://www.nbcnews.com/politics/national-security/dem-gop-senators-join-ask-trump-get-tough-russia-cyber-n894441

[12] T. B. Armstrong, A. G. Spitzer, B. S. Lucas, and M. G. White, "Transmission & distribution infrastructure," *A Harris Williams & Co. White Paper*, pp. 1–14, 2010.

[13] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inform. and Syst. Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.

[14] A. Sargolzaei, K. K. Yen, and M. N. Abdelghani, "Preventing time-delay switch attack on load frequency control in distributed power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 1176–1185, 2016.

[15] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, E. G. Im, B. Pranggono, and H. Wang, "Multiattribute SCADA-specific intrusion detection system for power networks," *IEEE Trans. Power Del.*, vol. 29, no. 3, pp. 1092–1102, 2014.

[16] Y. Zhang, L. Wang, W. Sun, R. C. Green II, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 796–808, 2011.

[17] H. Almakrami, "Intrusion detection system for smart meters," in *IEEE Saudi Arabia Smart Grid (SASG)*, 2016, pp. 1–8.

[18] J. Valenzuela, J. Wang, and N. Bissinger, "Real-time intrusion detection in power system operations," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1052–1062, 2013.

[19] M. Jamei, A. Scaglione, C. Roberts, E. Stewart, S. Peisert, C. McParland, and A. McEachern, "Anomaly detection using optimally-placed μpmu sensors in distribution grids," *IEEE Trans. Power Syst.*, vol. pp, no. pp, pp. 1–12, 2017.

[20] S. Pan, T. Morris, and U. Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 3104–3113, 2015.

[21] Y. Chen, L. Xie, and P. Kumar, "Dimensionality reduction and early event detection using online synchrophasor data," in *IEEE Power & Energy (PES) Soc. General Meeting*, 2013, pp. 1–5.

[22] L. Xie, Y. Chen, and P. R. Kumar, "Dimensionality reduction of synchrophasor data for early event detection: Linearized analysis," *IEEE Trans. Power Syst.*, vol. 29, no. 6, pp. 2784–2794, 2014.

[23] J. Valenzuela, J. Wang, and N. Bissinger, "Real-time intrusion detection in power system operations," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1052–1062, 2013.

[24] Y. Ge, A. J. Flueck, D.-K. Kim, J.-B. Ahn, J.-D. Lee, and D.-Y. Kwon, "Power system real-time event detection and associated data archival reduction based on synchrophasors," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 2088–2097, 2015.

[25] A. Allen, M. Singh, E. Muljadi, and S. Santoso, "Pmu data event detection: A user guide for power engineers," Nat. Renewable Energy Lab. (NREL), Tech. Rep., 2014.

[26] M. Biswal, S. M. Brahma, and H. Cao, "Supervisory protection and automated event diagnosis using pmu data," *IEEE Trans. Power Del.*, vol. 31, no. 4, pp. 1855–1863, 2016.

[27] M. Jamei, E. Stewart, S. Peisert, A. Scaglione, C. McParland, C. Roberts, and A. McEachern, "Micro synchrophasor-based intrusion detection in automated distribution systems: Toward critical infrastructure security," *IEEE Internet Computing*, vol. 20, no. 5, pp. 18–27, 2016.

[28] S. Brahma, R. Kavasseri, H. Cao, N. Chaudhuri, T. Alexopoulos, and Y. Cui, "Real-time identification of dynamic events in power systems using PMU data, and potential applicationsmodels, promises, and challenges," *IEEE Trans. Power Del.*, vol. 32, no. 1, pp. 294–301, 2017.

[29] (July 2018) What is Snort? [Online]. Available: https://www.snort.org/faq/what-is-snort

[30] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in distributed power systems," *Proc. of the IEEE*, vol. 105, no. 7, pp. 1367–1388, 2017.

[31] C. Wang, R. Callan, A. Zajic, and M. Prvulovic, "An algorithm for finding carriers of amplitude-modulated electromagnetic emanations in computer systems," in *IEEE 10th European Conf. on Antennas and Propag. (EuCAP)*, 2016, pp. 1–5.

[32] M. Prvulovic, A. Zajić, R. L. Callan, and C. J. Wang, "A method for finding frequency-modulated and amplitude-modulated electromagnetic emanations in computer systems," *IEEE Trans. Electromagn. Compat.*, vol. 59, no. 1, pp. 34–42, 2017.

[33] C. Bayens, T. Le, L. Garcia, R. Beyah, M. Javanmard, and S. Zonouz, "See no evil, hear no evil, feel no evil, print no evil? malicious fill patterns detection in additive manufacturing," *Proc. of the 26th USENIX Security Symp.*, pp. 1–18, 2017.

[34] Y. Han, S. Etigowni, H. Liu, S. Zonouz, and A. Petropulu, "Watch me, but don't touch me! contactless control flow monitoring via electromagnetic emanations," in *ACM Conf. on Computer and Communications Security (CCS)*, 2017, pp. 1095–1108.

[35] A. Nazari, N. Sehatbakhsh, M. Alam, A. Zajic, and M. Prvulovic, "Eddie: Em-based detection of deviations in program execution," in *ACM/IEEE 44th Annu. Int. Symp. Computer Architecture (ISCA)*, 2017, pp. 333–346.

[36] C. Cheng, S. Kim, and A. Zajic, "Comparison of path loss models for indoor 30 ghz, 140 ghz, and 300 ghz channels," in *11th European Conf. Antennas and Propag. (EUCAP)*, March 2017, pp. 716–720.

[37] S. M. Kaplan, "Electric power transmission: background and policy issues," *US Congressional Research Service*, vol. 14, pp. 4–5, 2009.

[38] K.-P. Brand, V. Lohmann, and W. Wimmer, *Substation automation handbook*. Utility Automation Consulting Lohmann Bremgarten, Switzerland, 2003.

[39] J. E. Sullivan and D. Kamensky, "How cyber-attacks in Ukraine show the vulnerability of the US power grid," *The Electricity J.*, vol. 30, no. 3, pp. 30–35, 2017.

[40] Vulnerability# ICS-VU-255987. Advisory (ICSA-17-089-02). (March 2017) Schneider Electric Modicon M221, M241, and M251 Programmable Logic Controllers (PLCs) TCP Predictability Vulnerability, Insufficiently Random/Shared Session Numbers Vulnerability, and Insufficiently Protected Credentials Vulnerability. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-17-089-02

[41] Vulnerability# ICS-VU-794684. Advisory (ICSA-16-070-01). (March 2016) Schneider Electric Telvent RTU Improper Ethernet Frame Padding Vulnerability. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-16-070-01

[42] Vulnerability# ICS-VU-130124. Advisory (ICSA-15-300-01). (October 2015) Siemens RuggedCom Improper Ethernet Frame Padding Vulnerability. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-15-300-01

[43] Vulnerability# ICS-VU-435619. Advisory (ICSA-15-006-01). (July 2015) Eaton's Cooper Power Series Form 6 Control and Idea/IdeaPLUS Relays with Ethernet Vulnerability. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-15-006-01

[44] Vulnerability# ICS-VU-532813. Advisory (ICSA-15-169-01). (June 2015) Wind River VxWorks TCP Predictability Vulnerability in ICS Devices. Vendor: Wind River (vendors affected - Schneider Electric). [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-15-169-01

[45] A. A. Ghirardi, *Radio Physics Course*. Radio Technical Publishing Company, 1932.

[46] M. B. Cohen, U. S. Inan, and E. W. Paschal, "Sensitive broadband ELF/VLF radio reception with the AWESOME instrument," *IEEE Trans. Geosci. Remote Sens.*, vol. 48, no. 1, pp. 3–17, 2010.

[47] M. B. Cohen, "ELF/VLF phased array generation via frequency-matched steering of a continuous hf ionospheric heating beam," Ph.D. dissertation, Stanford University, 2009.

[48] (July 2018) National Lightning Detection Network (NLDN). [Online]. Available: https://www.vaisala.com/en/products/data-subscriptions-and-reports/data-sets/nldn

[49] M. B. Cohen, R. Said, and U. Inan, "Mitigation of 50–60 hz power line interference in geophysical data," *Radio Science*, vol. 45, no. 6, 2010.

[50] T. Strutz, *Data fitting and uncertainty: A practical introduction to weighted least squares and beyond*. Vieweg and Teubner, 2010.

[51] (August 2018) Choptank Electric Cooperative. [Online]. Available: http://choptankelectric.com/

[52] (August 2018) Georgia Power. [Online]. Available: https://www.georgiapower.com/

[53] G. Barchi, D. Macii, D. Belega, and D. Petri, "Performance of synchrophasor estimators in transient conditions: A comparative analysis," *IEEE Trans. Instrum. Meas.*, vol. 62, no. 9, pp. 2410–2418, 2013.

[54] G. Barchi, D. Macii, and D. Petri, "Synchrophasor estimators accuracy: A comparative analysis," *IEEE Trans. Instrum. Meas.*, vol. 62, no. 5, pp. 963–973, 2013.

[55] R. A. Serrano and E. Halper, "Sophisticated but low-tech power grid attack baffles authorities," *Los Angeles Times*, vol. 11, 2014.

[56] A. R. Bergen and V. Vittal, *Power system analysis*. Upper Saddle River, NJ: Prentice-Hall, 2000.

[57] T. Shekari, F. Aminifar, and M. Sanaye-Pasand, "An analytical adaptive load shedding scheme against severe combinational disturbances," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 4135–4143, 2016.